(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-48479
(P2004-48479A)
(43)公開日　平成16年2月12日(2004.2.12)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/08	H04L	9/00	601Z	5B085
G06F 15/00	G06F	15/00	330A	5J104
	H04L	9/00	601F	

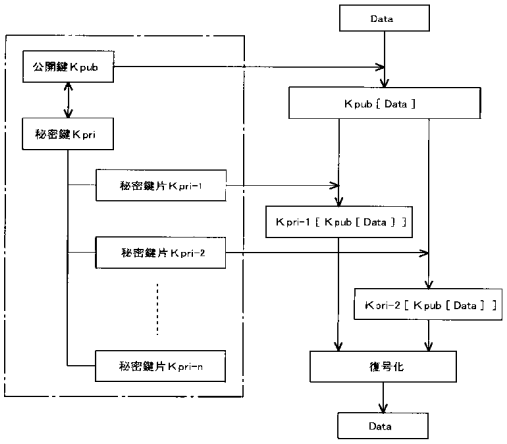
審査請求 未請求　請求項の数 6　OL　（全 9 頁）

(21)出願番号　特願2002-204495(P2002-204495)
(22)出願日　平成14年7月12日(2002.7.12)

(71)出願人　000208891
ＫＤＤＩ株式会社
東京都新宿区西新宿二丁目３番２号
(74)代理人　100084870
弁理士　田中　香樹
(74)代理人　100079289
弁理士　平木　道人
(74)代理人　100119688
弁理士　田邊　壽二
(72)発明者　三宅　優
埼玉県上福岡市大原二丁目１番１５号　株式会社ケイディーディーアイ研究所内
(72)発明者　中尾　康二
埼玉県上福岡市大原二丁目１番１５号　株式会社ケイディーディーアイ研究所内
最終頁に続く

(54)【発明の名称】共有化された暗号化情報の暗号鍵管理方法

(57)【要約】
【課題】共有情報の秘匿性が高く、暗号鍵の交換を容易かつ安全に行える、共有化された暗号化情報の暗号鍵管理方法を提供する。
【解決手段】公開鍵暗号の秘密鍵ＫＰｒｉを、　値暗号系のアルゴリズムを用いて複数の秘密鍵片ＫＰｒｉ－１，ＫＰｒｉ－２　ＫＰｒｉ－ｎに分割し、公開鍵ＫＰｕｂで暗号化された情報ＫＰｕｂ［Ｄａｔａ］を、　値として定められた数（本発明では、２つ）の秘密鍵片ＫＰｒｉ－１，ＫＰｒｉ－２を利用して、それぞれ別の場所で復号化することにより不完全な復号化情報ＫＰｒｉ－１［ＫＰｕｂ［Ｄａｔａ］］，ＫＰｒｉ－２［ＫＰｕｂ［Ｄａｔａ］］を生成し、これらをアクセスが許可された場所へ集めて情報Ｄａｔａを再生する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
暗号化された情報を記憶する計算機と複数のメンバー端末とがネットワークを介して接続され、各メンバー端末が前記計算機上で暗号化情報を共有するための暗号鍵管理方法において、
公開鍵暗号の秘密鍵を複数の秘密鍵片に分割し、公開鍵で暗号化された情報を複数の秘密鍵片を用いて復号化する　値暗号系の秘密分散共有方式を採用し、
複数のメンバー端末のいずれかが、
秘密鍵を分割して複数の秘密鍵片を生成する手順と、
公開鍵を各メンバー端末に配布する手順と、
各秘密鍵片を各メンバー端末および計算機に配布する手順と、
を予め実行し、
共有情報を提供するメンバー端末が、
前記共有情報を公開鍵で暗号化して暗号化情報を生成する手順と、
前記暗号化情報を前記計算機へ転送する手順と、
を実行することを特徴とする共有化された暗号化情報の暗号鍵管理方法。
【請求項２】
暗号化された情報を記憶する計算機と複数のメンバー端末とがネットワークを介して接続され、各メンバー端末が前記計算機上で暗号化情報を共有するための暗号鍵管理方法において、
公開鍵暗号の秘密鍵を複数の秘密鍵片に分割し、公開鍵で暗号化された情報を複数の秘密鍵片を用いて復号化する　値暗号系の秘密分散共有方式を採用し、
複数のメンバー端末のいずれかが、
秘密鍵を分割して複数の秘密鍵片を生成する手順と、
公開鍵を各メンバー端末に配布する手順と、
各秘密鍵片を各メンバー端末および計算機に配布する手順と、
を予め実行し、
前記計算機が、
公開鍵で暗号化された暗号化情報を、いずれかのメンバー端末から受信して記憶する手順と、
前記暗号化情報を、自身に配布されている秘密鍵片で不完全に復号化して第１の不完全復号化情報を生成する手順とを実行することを特徴とする共有化された暗号化情報の暗号鍵管理方法。
【請求項３】
暗号化された情報を記憶する計算機と複数のメンバー端末とがネットワークを介して接続され、各メンバー端末が前記計算機上で暗号化情報を共有するための暗号鍵管理方法において、
公開鍵暗号の秘密鍵を複数の秘密鍵片に分割し、公開鍵で暗号化された情報を複数の秘密鍵片を用いて復号化する　値暗号系の秘密分散共有方式を採用し、
複数のメンバー端末のいずれかが、
秘密鍵を分割して複数の秘密鍵片を生成する手順と、
公開鍵を各メンバー端末に配布する手順と、
各秘密鍵片を各メンバー端末および計算機に配布する手順と、
を予め実行し、
メンバー端末が、
前記計算機から、前記公開鍵で暗号化された暗号化情報、および当該暗号化情報を計算機が自信の秘密鍵片で不完全に復号化して得た第１の不完全復号化情報を取得する手順と、
前記取得した暗号化情報を、自身に配布されている秘密鍵片で不完全に復号化して第２の不完全復号化情報を生成する手順と、
前記第１および第２の不完全復号化情報に基づいて共有情報を再生する手順と、を実行す

ることを特徴とする共有化された暗号化情報の暗号鍵管理方法。
【請求項４】
暗号化された情報を記憶する計算機と複数のメンバー端末とがネットワークを介して接続され、各メンバー端末が前記計算機上で暗号化情報を共有するための暗号鍵管理方法において、
公開鍵暗号の秘密鍵を複数の秘密鍵片に分割し、公開鍵で暗号化された情報を複数の秘密鍵片を用いて復号化する　値暗号系の秘密分散共有方式を採用し、
複数のメンバー端末のいずれかが、
秘密鍵を分割して複数の秘密鍵片を生成する手順と、
公開鍵を各メンバー端末に配布する手順と、
各秘密鍵片を各メンバー端末および計算機に配布する手順と、
を予め実行し、
共有情報を提供するメンバー端末が、
前記共有情報を公開鍵で暗号化して暗号化情報を生成する手順と、
前記暗号化情報を前記計算機へ転送する手順と、
を実行し、
前記計算機が、
前記暗号化情報を受信して記憶する手順と、
前記暗号化情報を、自身に配布されている秘密鍵片で不完全に復号化して第１の不完全復号化情報を生成する手順と、
を実行し、
共有情報を取得するメンバー端末が、
前記計算機から、前記暗号化情報および第１の不完全復号化情報を取得する手順と、
前記取得した暗号化情報を、自身に配布されている秘密鍵片で不完全に復号化して第２の不完全復号化情報を生成する手順と、
前記第１および第２の不完全復号化情報に基づいて共有情報を再生する手順と、を実行することを特徴とする共有化された暗号化情報の暗号鍵管理方法。
【請求項５】
前記秘密鍵片が、前記秘密鍵と乱数組Ｒとに基づいて生成されることを特徴とする請求項４に記載の共有化された暗号化情報の暗号鍵管理方法。
【請求項６】
前記秘密鍵片を、前記秘密鍵と他の乱数組Ｒ’とに基づいて再生成する手順と、
前記再生成された各秘密鍵片を各メンバー端末および計算機に再配布する手順と、
前記各メンバー端末および計算機が、既登録の秘密鍵片を前記再配布された秘密鍵片に置換する手順とを含むことを特徴とする請求項５に記載の共有化された暗号化情報の暗号鍵管理方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、インターネット等のネットワーク上に設置された計算機（データサーバ）を利用して、重要な情報を複数のメンバーが共有するための暗号鍵管理方法に係り、特に、共有情報の秘密性を高度に維持しながら、暗号鍵の交換を容易にした暗号鍵管理方法に関する。
【０００２】
【従来の技術】近年、通信分野において、伝送される情報の秘密性を保護する技術として各種の暗号化技術が提案されている。
【０００３】
ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）では、通信路、すなわちサーバにアクセスするメンバーが利用するメンバー端末とサーバとの間の通信が暗号化される。利用者が送信したデータは、インターネット等のネットワーク上では暗号化されて送信され

るため、ネットワークを監視していても、その中身を知ることは不可能である。
【０００４】
しかしながら、メンバーが送信した情報（データ）は、サーバに到着した時点で復号化され、誰でも読める形式で保管される。このため、サーバを管理している管理者は、労せずして秘密情報を盗み見ることができる。
【０００５】
また、この種のサーバは誰もがアクセスできるネットワーク上に設置されることが多いため、不正アクセスによるサーバへの侵入により、そこに保管されている秘匿情報が漏れてしまう事件も発生している。
【０００６】
これに対して、データベース自体を暗号化する手法として、データベースやファイルシステムに暗号化機能を組み込むことにより、保管されている秘匿情報を保護する装置が普及している。これにより、何らかの方法で暗号化されたデータにアクセスできたとしても、これに対応する暗号鍵が無ければ情報へのアクセスは不可能となる。しかしながら、一つの暗号鍵を複数のメンバーが共有することは安全上好ましくなく、以下のような問題が発生する。
【０００７】
▲１▼情報を共有するメンバー全員に同じ暗号鍵が配布された場合、暗号鍵が漏れても誰から漏れたかの判断ができない。
【０００８】
▲２▼情報を共有するメンバーの構成が変更され、今までアクセスを許可されていたメンバーのアクセス権を剥奪する場合、電子的に配布された暗号鍵を取り上げるわけには行かない。
【０００９】
▲３▼暗号鍵を変更する場合には、サーバ上に保管されている秘匿情報の暗号化をやり直す必要がある。このとき、古い暗号鍵で情報を復号して元に戻し、新しい暗号鍵で暗号化する必要があるため、保管されている情報が多い場合には、この処理に時間を要する。
【００１０】
▲４▼上記した暗号化のやり直しをサーバ上で行おうとすれば、古い暗号鍵と新しい暗号鍵の両方をサーバに登録する必要があるため、暗号鍵がサーバの管理者やサーバへの侵入者に渡る可能性がある。
【００１１】
▲５▼上記した暗号化のやり直しをサーバ外で行おうとすれと、古い暗号鍵と新しい暗号鍵とを持つメンバーがサーバから情報を取り出して復号化し、これを新しい暗号鍵で再度暗号化してサーバ上の情報に上書きする必要がある。このため、ネットワークのトラフィックを著しく増大させるのみならず、暗号化処理のために強力な計算機が必要となる。
【００１２】
本発明の目的は、上記した従来技術の課題を解決し、共有情報の秘匿性が高く、暗号鍵の交換を容易かつ安全に行える共有化された暗号化情報の暗号鍵管理方法を提供することにある。
【００１３】
【課題を解決するための手段】
上記した目的を達成するために、本発明は、暗号化された情報を記憶する計算機と複数のメンバー端末とがネットワークを介して接続され、複数のメンバーが前記計算機上で暗号化情報を共有するための暗号鍵管理方法において、以下のような手順を含むことを特徴とする。
（１）公開鍵暗号の秘密鍵を複数の秘密鍵片に分割し、公開鍵で暗号化された情報を複数の秘密鍵片を用いて復号化する　値暗号系の秘密分散共有方式を採用すること。
（２）秘密鍵を分割して複数の秘密鍵片を生成すること。
（３）予め公開鍵を各メンバー端末に配布し、各秘密鍵片を各メンバー端末および計算機

に配布すること。
（４）共有情報を提供するメンバー端末が、共有情報を公開鍵で暗号化して暗号化情報を生成し、これを計算機へ転送すること。
（５）計算機が、暗号化情報を受信して記憶し、この暗号化情報を、自身に配布されている秘密鍵片で不完全に復号化して第１の不完全復号化情報を生成すること。
（６）共有情報を取得するメンバー端末が、計算機から暗号化情報および第１の不完全復号化情報を取得し、取得した暗号化情報を、自身に配布されている秘密鍵片で不完全に復号化して第２の不完全復号化情報を生成し、第１および第２の不完全復号化情報に基づいて共有情報を再生すること。
【００１４】
上記した特徴によれば、以下のような作用効果が奏せられる。
（ａ）各メンバー端末とデータサーバとを結ぶ通信路上のみならず、データサーバ上でも、共有情報は暗号化された状態で保持されるので、その安全性が向上する。
（ｂ）各メンバーに配布している秘密鍵片を変更する場合でも、秘密鍵を作り直すことなく、秘密鍵片のみを作り直して再配布すれば良いので、共有情報を改めて暗号化し直す必要がない。
（ｃ）全ての秘密鍵片が相互に異なるので、秘密鍵片が漏洩した場合には、その漏洩元を容易に突き止めることができる。
【００１５】
【発明の実施の形態】
以下、図面を参照して本発明の好ましい実施の形態について詳細に説明する。初めに、本発明において採用するＲＳＡ（Ｒｉｖｅｓｔ　Ｓｈａｍｉｒ　Ａｄｌｅｍａｎ）値暗号系の秘密分散共有方式（Ｔｈｒｅｓｈｏｌｄ　ＣｒｙＰｔｏｇｒａＰｈｙ）について説明する。
【００１６】
一般の秘密分散共有方式では、公開鍵ＫＰｕｂで暗号化した情報を秘密鍵ＫＰｒｉで再生（復号化）する公開鍵方式の暗号化システムにおいて、秘密鍵ＫＰｒｉを複数の秘密鍵片ＫＰｒｉ－１，ＫＰｒｉ－２　ＫＰｒｉ－ｎに分割して複数の管理者が保管する。暗号解読時には、秘密鍵片の全部、または　値として定められた数の秘密鍵片で秘密鍵ＫＰｒｉを再生し、この秘密鍵で暗号化情報を再生する。
【００１７】
これに対して、本発明が採用するＲＳＡ　値暗号系では、図１に示したように、公開鍵暗号の秘密鍵ＫＰｒｉを、　値暗号系のアルゴリズムを用いて複数の秘密鍵片ＫＰｒｉ－１，ＫＰｒｉ－２　ＫＰｒｉ－ｎに分割する。各秘密鍵片は、そのうちのいずれか複数が揃えば秘密鍵ＫＰｒｉと同等の機能を発揮することができる。そして、公開鍵ＫＰｕｂで暗号化された情報ＫＰｕｂ［Ｄａｔａ］を、　値として定められた数（本発明では、２つ）の秘密鍵片ＫＰｒｉ－１，ＫＰｒｉ－２で別々に復号化して不完全な複合化情報ＫＰｒｉ－１［ＫＰｕｂ［Ｄａｔａ］］，ＫＰｒｉ－２［ＫＰｕｂ［Ｄａｔａ］］を生成し、この２つを用いて情報Ｄａｔａを再生する。したがって、ここでは秘密鍵ＫＰｒｉを再生する必要がない。
【００１８】
なお、このような秘密分散共有法を適用した暗号化手法に関しては、「臨時別冊・数理科学『現代暗号とマジックプロトコル』」（今井秀樹編著；株式会社サイエンス社；２０００年９月２５日発行）において、「秘密分散共有法」と題して論じられている。
【００１９】
次いで、図２－８のブロック図および図９のシーケンス図を参照しながら、本実施形態の動作を詳細に説明する。
【００２０】
図２において、複数のメンバー１～ｎの各メンバー端末Ｎ１～Ｎｎとデータサーバ ＤＳとはインターネットを介して相互に接続されている。本実施形態では、メンバー１のメンバ

ー端末Ｎ１が主端末として機能し、公開鍵ＫＰｕｂおよび秘密鍵ＫＰｒｉを管理すると共に、秘密鍵ＫＰｒｉとパラメータとしての乱数組Ｒとに基づいて、予め複数個（本実施形態では、メンバー端末数ｎとデータサーバ数との総和；ｎ＋１）の秘密鍵片ＫＰｒｉ－１～ＫＰｒｉ－ｎ，ＫＰｒｉ－Ｓを生成する［図９のステップＳ１］。

【００２１】

主端末Ｎ１は、図３に示したように、公開鍵ＫＰｕｂを全てのメンバー端末Ｎ２～Ｎｎへ配布すると共に、秘密鍵片ＫＰｒｉ－２～ＫＰｒｉ－ｎ，ＫＰｒｉ－ＳをデータサーバＤＳおよび各メンバー端末Ｎ２～Ｎｎへ配布する［ステップＳ２］。

【００２２】

データサーバＤＳおよび各メンバー端末Ｎ２～Ｎｎは、配布された公開鍵ＫＰｕｂおよび秘密鍵片ＫＰｒｉ－２～ＫＰｒｉ－ｎ，ＫＰｒｉ－Ｓを自身に登録する［図９のステップＳ３，４，５］。メンバー端末Ｎ１は、秘密鍵片ＫＰｒｉ－１を自信に固有の秘密鍵片として記憶する。

【００２３】

その後、例えばメンバー端末Ｎ１が共有情報Ｄａｔａをデータサーバ ＤＳへ登録する場合、図４に示したように、共有情報Ｄａｔａを公開鍵ＫＰｕｂで暗号化し［図９のステップＳ６］、さらに、この暗号化情報ＫＰｕｂ［Ｄａｔａ］をデータサーバＤＳへ転送する［ステップＳ７］。

【００２４】

データサーバＤＳは、暗号化情報ＫＰｕｂ［Ｄａｔａ］を受信すると［ステップＳ８］、図５に示したように、この暗号化情報ＫＰｕｂ［Ｄａｔａ］を自身の秘密鍵片ＫＰｒｉ－Ｓで不完全に復号化して、不完全な復号化情報ＫＰｒｉ－Ｓ［ＫＰｕｂ［Ｄａｔａ］］を生成し［ステップＳ９］、これを登録する［ステップＳ１０］。

【００２５】

その後、例えばメンバー端末Ｎ２が共有情報Ｄａｔａを利用する場合、データサーバＤＳから前記暗号化情報ＫＰｕｂ［Ｄａｔａ］および不完全な復号化情報ＫＰｒｉ－Ｓ［ＫＰｕｂ［Ｄａｔａ］］を取得する［ステップＳ１１］。次いで、図６に示したように、暗号化情報ＫＰｕｂ［Ｄａｔａ］を自身の秘密鍵片ＫＰｒｉ－２で復号化して、不完全な復号化情報ＫＰｒｉ－２［ＫＰｕｂ［Ｄａｔａ］］を生成する［ステップＳ１２］。最後に、この２つの不完全な復号化情報ＫＰｒｉ－Ｓ［ＫＰｕｂ［Ｄａｔａ］］およびＫＰｒｉ－２［ＫＰｕｂ［Ｄａｔａ］］に基づいて共有情報Ｄａｔａを再生する［ステップＳ１３］。

【００２６】

このように、本実施形態によれば、各メンバー端末ＮとデータサーバＤＳとを結ぶ通信路上のみならず、データサーバＤＳ上でも共有情報Ｄａｔａが暗号化された状態に保持されるので、その安全性が向上する。

【００２７】

なお、メンバーの入れ替わり等により秘密鍵片を交換する場合、本実施形態では、図７に示したように、主端末Ｎ１が前記乱数組Ｒと異なる他の乱数組Ｒ’と秘密鍵ＫＰｒｉとに基づいて秘密鍵片Ｋ’Ｐｒｉ－１～Ｋ’Ｐｒｉ－ｎ，Ｋ’Ｐｒｉ－Ｓを新規に生成し、図８に示したように、この秘密鍵片Ｋ’Ｐｒｉ－１～Ｋ’Ｐｒｉ－ｎ，Ｋ’Ｐｒｉ－Ｓのみをデータサーバ ＤＳおよび各メンバー端末Ｎ２～Ｎｎへ配布して差し替える。

【００２８】

このように、本実施形態によれば、各メンバーに配布している秘密鍵片を変更する場合でも、秘密鍵を作り直すことなく、秘密鍵片のみを作り直して再配布すれば良いので、共有情報を改めて暗号化し直す必要がない。しかも、本実施形態によれば、新たな秘密鍵片は、秘密鍵を分割する際のパラメータ（乱数組）を変更するのみで生成できるので、秘密鍵片の変更が容易になる。

【００２９】

さらに、本実施形態によれば、全ての秘密鍵片が相互に異なるので、秘密鍵片が漏洩した

場合には、その漏洩元を容易に突き止めることができる。

【００３０】

【発明の効果】本発明によれば、以下のような効果が達成される。

（１）各メンバー端末とデータサーバとを結ぶ通信路上のみならず、データサーバ上でも共有情報が暗号化された状態に保持されるので、その安全性が向上する。（２）各メンバーに配布している秘密鍵片を新しい秘密鍵片と入れ替える場合でも、秘密鍵を作り直すことなく、秘密鍵を秘密鍵片に分割する際のパラメータのみを変更すれば良いので、共有情報を改めて暗号化し直す必要がない。

（３）全ての秘密鍵片が相互に異なるので、秘密鍵片が漏洩した場合でも、その漏洩元を容易に突き止めることができる。

【図面の簡単な説明】

【図１】ＲＳＡ　値暗号系の秘密分散共有方式を説明するためのブロック図である。

【図２】本発明の暗号鍵管理方法を説明するためのブロック図（その１）である。

【図３】本発明の暗号鍵管理方法を説明するためのブロック図（その２）である。

【図４】本発明の暗号鍵管理方法を説明するためのブロック図（その３）である。

【図５】本発明の暗号鍵管理方法を説明するためのブロック図（その４）である。

【図６】本発明の暗号鍵管理方法を説明するためのブロック図（その５）である。

【図７】本発明の暗号鍵管理方法を説明するためのブロック図（その６）である。

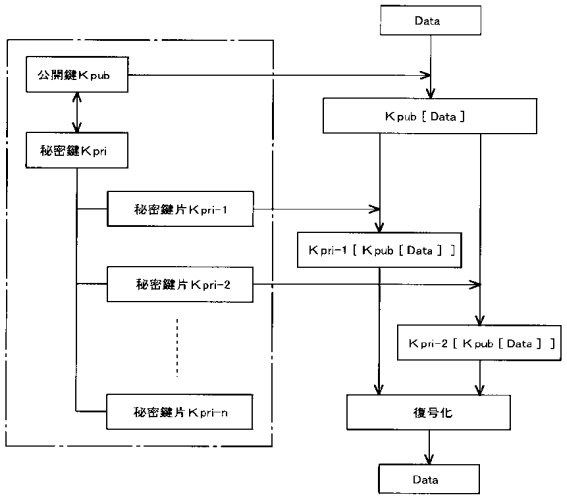
【図８】本発明の暗号鍵管理方法を説明するためのブロック図（その７）である。

【図９】本発明の暗号鍵管理方法を示した１シーケンス図である。

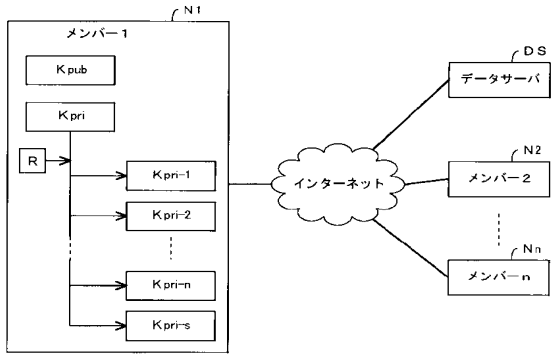
【符号の説明】

Ｎ１～Ｎｎ　メンバー端末，ＤＳ　データサーバ

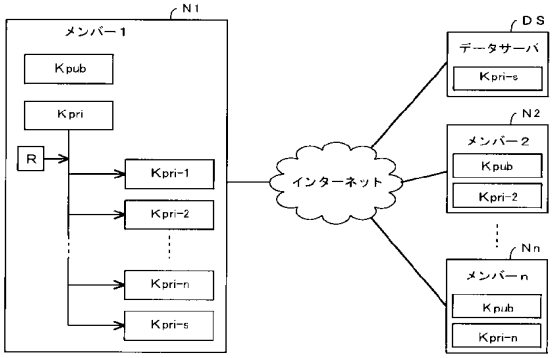
【図１】



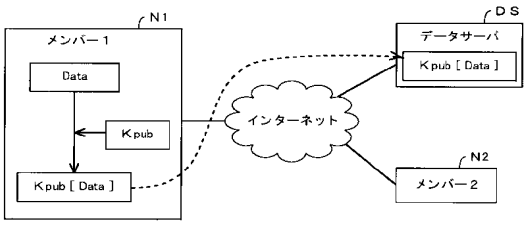
【図２】



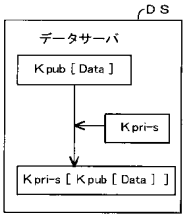
【図３】



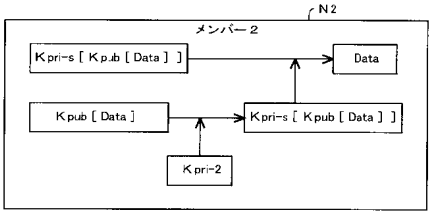
【図４】



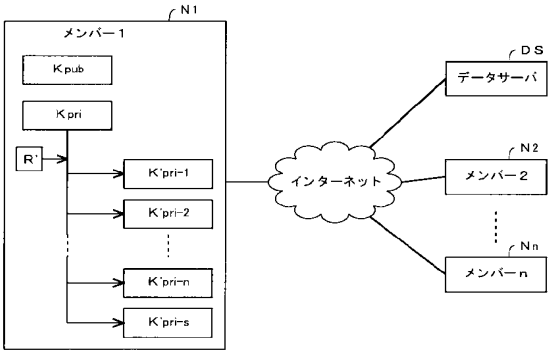
【図５】



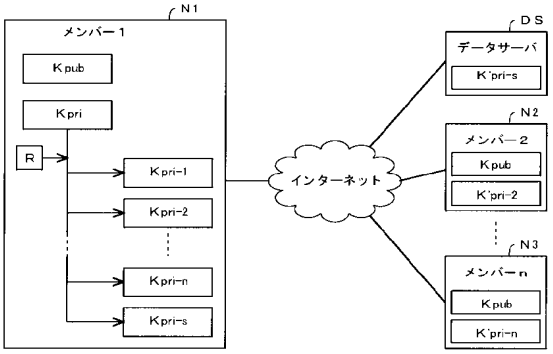
【図６】



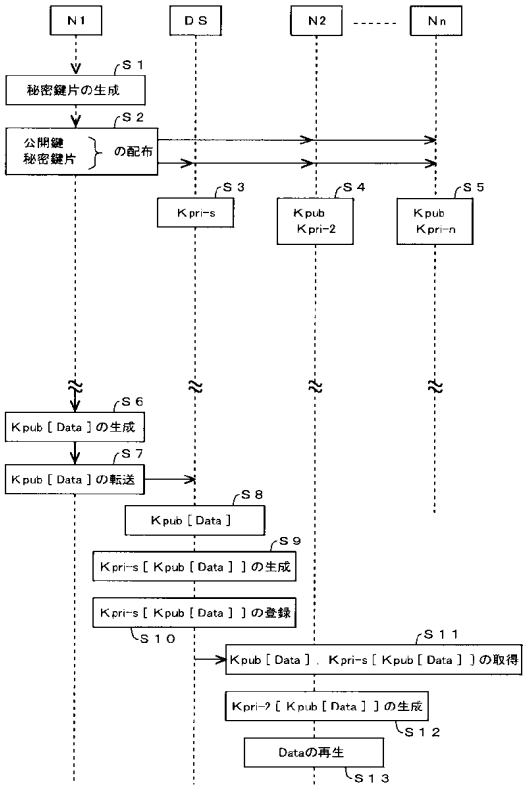
【図７】



【図８】



【図９】



フロントページの続き

Fターム(参考) 5B085 AA08 AE29 BA06 BG02
5J104 AA16 EA04 EA15 EA19 NA02 PA07